This is a 3-credit course that focuses on security applications and cryptographic protocols. An overview of cryptography will be given in the first couple of weeks.


Prerequisite: Students are expected to come with undergrad level computer networks and operating systems background. Moreover, computer-programming expertise is necessary. CS408 or TE404 is prerequisite. However, if you have not taken one of these courses but have a background on Computer Networks, feel free to inquiry with the instructor for any possible prerequisite override

Instructor: Albert Levi
FENS 1091, x9563, levi at sabanciuniv edu

Assistants: N.Alperen Pulur, Dilara Akdoğan

Schedule: Lecture: T 9:40 – 10:30 FENS G032 and Th 12:40 – 14:30, FASS G022
Lab/Recitation: T 17:40 – 19:30, FASS G022 (note the room change) (both sections will meet there) (we will not use this hour all the time; you will be informed when there is recitation/lab through lab website)


Reference: Computer Security, Dieter Gollmann

Tentative Outline
- Introduction (1 week)
- Overview of Cryptography (2-3 weeks)
  - Symmetric and Asymmetric Cryptography
  - Key agreement
  - Hash functions
- Authentication and Key Distribution Protocols (1-2 weeks)
- Kerberos and Password Management (1 week)
- TCP/IP Security and IPsec (2 weeks)
- WWW Security, SSL and TLS (1 week)
- E-mail Security (PGP, S/MIME, Domainkeys) (2 weeks)
- PKI and certificate systems, (1 week)
- Access Control (1 week)
- Firewalls and Intrusion Detection Systems (1-2 weeks)

Make-up Policy: No make-up! If you miss something, you miss it whatever the reason is!

Student responsibilities and loads (tentative)
- One in-class midterm and one in-class final exam.
- There will be 5 (+/- 1) labs. The labs will be dedicated to some practical aspects of the course including programming. Labs will be graded either as in-lab performance or as a separate homework or as after-lab performance. Aside the lab homework assignments there will 1-2 lecture related homework assignments. Some homework assignments may require programming. This year we will organize Capture the Flag (CtF) contest as part of homework.
- A programming project on a secure networking application. This project will be done in 2 or 3 stages and you will be able to work in groups of at most 2 people.

Tentative Grading and Timing
Midterm Exam 25-30%  April 14, 2015, Tuesday, 17:40-19:30 (lab/recitation hour)  week 10
Final Exam 35-40%  as scheduled by ÖK/SR
Homework, Lab, Project, CtF 30-40%  deadlines will be determined separately

Class Website: http://people.sabanciuniv.edu/levi/cs432

PLAGIARISM WILL NOT BE TOLERATED